Performance analysis of quantum key distribution in underwater turbulence channels

Performance Analysis of Quantum Key Distribution in Underwater Turbulence Channels

Amir Hossein Fahim Raouf[1], Majid Safari[2], and Murat Uysal[1]

[1]Department of Electrical and Electronics Engineering
Ozyegin University, Istanbul, Turkey, 34794

[2]Institute for Digital Communications,
University of Edinburgh, Edinburgh EH3 9JL, U.K.

E-mails: amirh.fraouf@ieee.org, majid.safari@ed.ac.uk, murat.uysal@ozyegin.edu.tr

Abstract **–**The current literature on quantum key distribution (QKD) is mainly limited to the transmissions over fiber optic, atmospheric or satellite links and are not directly applicable to underwater environments with different channel characteristics. In this paper, we analyze the quantum bit error rate (QBER) and secret key rate (SKR) performance of the well-known BB84 protocol in underwater channels. As path loss model, we consider a modified version of Beer-Lambert formula which takes into account the effect of scattering. We derive a closed-form expression for the wave structure function to determine the average power transfer over turbulent underwater path and use this to obtain an upper bound on QBER as well as a lower bound on SKR. Based on the derived bounds, we present the performance of BB84 protocol in different water types including clear, coastal and turbid water and under different atmospheric conditions such as clear, hazy and overcast. We further investigate the effect of system parameters such as aperture size and detector field-of-view on QBER and SKR performance metrics.

Keywords **–** Quantum key distribution (QKD), quantum bit error rate (QBER), secret key rate (SKR), underwater turbulence

I. Introduction

Underwater sensor networks (USNs) [1] have emerged to provide an integrated system for the surveillance of critical maritime zones and infrastructures, see e.g., [2-3] for some commercially available solutions. With high density node deployment, USNs bring improved agility, resilience and fault tolerance. In addition, they introduce advantages including a higher probability of detection and classification, lower false alarm rate, and more accuracy in the localization of threats. Despite the increasing deployment of USNs and growing relevant literature, cyber security aspects of USNs have received relatively low attention. Particularly for maritime applications such as the surveillance of critical infrastructure and border protection, secure communication is the key to ensure the confidentiality, integrity and authentication of the transmitted information. Some countermeasures for cyber-attacks have been investigated for underwater wireless networks [4-6]. For example, a simple symmetric cryptosystem with CipherText Stealing technique is used in [4]. An energy-efficient secure message authentication protocol with the standard encryption techniques is employed in [5]. Similarly, the literature on underwater wireless networks, see e.g., the survey in [6] and references therein, focus only on conventional cryptosystems.

The new era of quantum computing brings the necessity of quantum-secure cryptography schemes. Based on the firm laws of physics rather than unproven foundations of mathematical complexity, quantum cryptography [7] promises unconditional security. Quantum key distribution (QKD) is used to produce a shared random secret key known only to sender and receiver parties. This key can then be used to encrypt a message, which is transmitted over a standard communication (acoustic, optical, radio, etc.) channel. The first QKD protocol proposed by Bennett and Brassard, today widely known as BB84 [8] is a prepare-and-measure (PaM) protocol where a qubit state is first prepared, then sent to the other party. Later, entanglement-based protocols [9-12] have emerged in which the two parties share a joint state and perform measurements on that. Although entanglement protocols offer an additional level of security as the quantum source does not have to be trusted, PaM protocols have been more popular mainly due to their simplicity. Most of QKD protocols are limited to binary signal

format, i.e., qubits, which are two-level quantum systems. To take advantage of the higher dimensionality, orbital angular momentum (OAM) is further used to design QKD systems [13-14]. In these systems, the encoded quantum states belong to a higher dimensional Hilbert space where qudits rather than qubits are used. The feasibility of various QKD protocols has been further demonstrated through successful experiments for different transmission ranges and data rates, see e.g., a recent survey [15] and references therein.

The current literature on QKD is mainly limited to the transmissions over fiber optic, atmospheric or satellite links and are not directly applicable to underwater environments with different channel characteristics. There have been only some recent efforts on underwater QKD [16-25]. For example, in [16] and [17], based on the well-known Beer-Lambert path loss model, the maximum secure communication distance for BB84 protocol in underwater environments was derived to achieve a desired level of quantum bit error rate (QBER) and the secret key rate (SKR). In [18] and [19], Monte Carlo simulations were conducted to determine the propagation characteristics of polarized photons in the underwater channel. Using these simulated underwater channels, the QBER performance of BB84 QKD protocol was computed. Some experimental demonstrations of underwater QKD were further reported in [20-22] using aquariums and water tanks. Specifically, in [20], Bouchard et al. implemented 2- and 3-dimensional BB84 protocols and reported results for a transmission distance of 3 meters. In another experiment over a 2.37 m distance [21], Zhao et al. reported that QBER less than 3.5% can be achieved for different water types with extinction coefficients up to 0.7 m^{-1}. In [22], Hu et al. used a semi-open water tank and experimentally verified the feasibility of underwater QKD over a transmission distance of 55 meters.

The above theoretical and experimental works consider only the path loss, but ignore the effects of turbulence. In practical scenarios, rapid changes in the refractive index commonly caused by ocean currents induce sudden variations in the water temperature and pressure. This turbulence results in fluctuations of the optical signal known as fading. The effects of underwater turbulence on QKD systems were addressed only recently in [23-25]. In [23], Bouchard et al. experimentally investigated the effect of turbulence on an OAM-based QKD

system in an outdoor swimming pool exposed to temperatures in the range of 17 C - 27 C and demonstrated performance degradations due to turbulence. In [24], Hufnagel et al. carried out an experiment in Ottawa River for a 5.5 meter quantum link and quantified the effect of turbulence on optical beams with different polarization states and spatial modes. In [25], Gariano and Djordjevic adopted the split step beam propagation simulation method to model the effect of oceanic turbulence and used this model to calculate the SKR of BB84 protocol.

In this paper, we investigate the fundamental performance limits of BB84 protocol over turbulent underwater channels and provide a comprehensive performance characterization. As path loss model, we consider a modified version of Beer-Lambert formula, which takes into account the effect of scattering. We derive a closed-form expression for the wave structure function to determine the average power transfer over turbulent underwater path and use this to obtain an upper bound on QBER and a lower bound on SKR. Based on these bounds, we present the performance of BB84 protocol in different water types (clear, coastal and turbid) and different atmospheric conditions (clear, hazy and overcast atmosphere with relative locations of sun and earth at day time). We further investigate the effect of transmit aperture size and detector field-of-view (FOV) on the system performance.

The remainder of this paper is organized as follows. In Section II, we describe our system model based on BB84 QKD protocol. In Section III, we derive the underwater wave structure function and analyze the QBER and SKR in the presence of turbulence. In Section IV, we present numerical results to corroborate on the derived expressions. Finally, we conclude in Section V.

II. System Model

Fig. 1 illustrates a schematic diagram of a typical QKD system which uses BB84 protocol for key distribution. In this protocol, the authorized partners, Alice and Bob, wish to establish a secret key about which no eavesdropper (Eve) can acquire noteworthy information. Alice prepares a qubit by choosing randomly between two linear polarization bases $\oplus$ or $\otimes$ for every bit she wants to send. She selects a random bit value “0” or “1” for each chosen base, using the following polarization rule

$$\oplus \rightarrow \begin{cases} 0°, & \text{if "0" was chosen} \\ +90°, & \text{if "1" was chosen} \end{cases}$$

$$\otimes \rightarrow \begin{cases} -45°, & \text{if "0" was chosen} \\ +45°, & \text{if "1" was chosen} \end{cases}$$

At the receiver side, a passive 50:50 beam splitter chooses a random basis from the two bases. At the outputs of the beam splitter, two polarization detectors measure the quantum state of the possibly coming photon based on the two different bases. Each of these units includes a polarizing beam splitter (PBS) to decide between two orthogonal polarization states of the corresponding basis and two single-photon avalanche photodiodes (APDs) operating in Geiger-Mode for photon counting. Alice and Bob construct the secure key based on the qubits received at the "sift" events. Sift events correspond to the bit intervals in which exactly one of the APDs registers a count and both Alice and Bob have chosen the same basis. Alice and Bob can recognize the sift events by transferring information over a public classical communication channel (in our case underwater optical channel). In practice, in addition to Eve's potential intervention, the sifted key contains errors caused by path loss, turbulence and noise in Bob's detectors. Error correction is employed to reduce the effect of such channel imperfections [26].

Assume that Alice transmits a normalized spatial beam pattern from circular exit pupil and a diameter of d_1 with an average photon number of n_S to represent her bit value. Bob collects the light received from Alice with a diameter of d_2 in the $z = L$ plane. The effects of diffraction, turbulence and attenuation loss lead to a reduction in Bob's collected photons. In addition, Bob's receiver will collect n_B background photons per polarization on average, and each of his detectors will be subject to an average equivalent dark current photon number of n_D. By considering the dark current and irradiance of the environment, the average number of noise photons reaching each Bob's detector can be obtained by [27]

$$n_N = n_B/2 + n_D = I_{dc}\Delta t + \frac{1}{2}\frac{\pi R_d A \Delta t' \lambda \Delta\lambda \left(1-\cos(\Omega)\right)}{2h_p c_{light}} \tag{1}$$

where I_{dc} is the dark current count rate, A is the receiver aperture area, Ω is the FOV of the detector, h_p is Planck's constant, c_{light} is the speed of light, R_d is the irradiance of the environment, $\Delta\lambda$ is the filter spectral width, Δt is the bit period and $\Delta t'$ is the receiver gate time. It is convenient to write the depth dependence of $R_d(\lambda, z_d)$ as

$$R_d(\lambda, z_d) = R_d(\lambda, 0) e^{-K_\infty z_d} \tag{2}$$

where K_∞ is the asymptotic value of the spectral diffuse attenuation coefficient for spectral downwelling plane irradiance [28]. The typical total irradiances at sea level in the visible wavelength band for some atmospheric conditions are provided in [29].

III. Performance Analysis

In this section, we investigate the performance of the underwater QKD system through the derivation of an upper bound on QBER and a lower bound on SKR.

III.a. QBER Analysis

QBER is defined as the error rate in the sifted key. Mathematically speaking, it is given by [30]

$$\text{QBER} = \frac{\Pr(\text{error})}{\Pr(\text{sift})} \tag{3}$$

Replacing lower and upper bounds for sift and error probabilities obtained in [31] over a turbulent channel based on the near-field analysis, a lower bound on QBER is obtained as

$$\text{QBER} \le \frac{n_N\left(1-\mu+\mu e^{-\eta n_S l}\right)}{\frac{n_S l}{2}\mu e^{-\eta n_S l} + 2n_N\left(1-\mu+\mu e^{-\eta n_S l}\right)} \tag{4}$$

where η is the quantum efficiency of APDs, l is the path loss and μ is the average power transfer over the turbulent path. Calculation of l and μ depends on the operation environment and will be discussed in the following for the underwater channel under consideration.

The underwater path loss is a function of attenuation and geometrical losses. For collimated light sources, the geometrical loss is negligible; therefore, the path loss with a laser diode transmitter only depends on the attenuation loss. The attenuation loss is characterized by wavelength-dependent extinction coefficient $\varsigma = \alpha + \beta$ where α and β respectively denote absorption and scattering coefficients. Typical values of absorption and scattering coefficients for different water types including clear ocean, coastal water, and turbid harbor can be found in Table 1 for $\lambda = 532$ nm, i.e., in the blue-green spectral region [32]. In our work, we utilize

the modified version of Beer-Lambert formula proposed in [33], which takes into account the contribution of scattered lights. The path loss for a transmission distance of L can be given as

$$l = \exp\left[-\varsigma L \left(\frac{d_2}{\theta L} \right)^T \right] \tag{5}$$

where θ is full-width transmitter beam divergence angle and T is a correction coefficient [33].

The average power transfer over the turbulent path is expressed as [31]

$$\mu = \frac{8\sqrt{F}}{\pi} \int_0^1 \exp\left(-W\left(d_1 x, L\right)/2\right) \left(\cos^{-1}\left(x\right) - x\sqrt{1-x^2} \right) J_1\left(4x\sqrt{F}\right) dx \tag{6}$$

where F is the Fresnel number given by $F = \left(\left(\pi d_1 d_2\right)/4\lambda L \right)^2$ and $J_1(\bullet$ is the first-order Bessel function of the first kind. Here, $W(\bullet\bullet$ is the wave structure function and is related to spatial power spectrum of refractive index, therefore dependent on the operation environment. Let ρ denote the distance between two observation points. For spherical waves, wave structure function can be calculated as [34]

$$W\left(\rho, L\right) = 8\pi^2 k^2 L \int_0^1 \int_0^\infty \left[1 - J_0\left(\kappa\zeta\rho\right)\right] \Phi\left(\kappa\right) \kappa d\kappa d\zeta \tag{7}$$

where $J_0(\cdot)$ is the zero-order Bessel function and $\Phi\left(\kappa\right)$ is three-dimensional spatial power spectrum of refractive index in turbulent ocean. In the following, we derive a closed-form expression for underwater wave structure function.

Assume that ε denotes the dissipation rate of turbulent kinetic energy per unit mass of fluid. Let α_{th} and χ_T respectively denote the thermal expansion coefficient and the dissipation rate of mean-squared temperature. Furthermore, let d_r denote the eddy diffusivity ratio. Based on the modified Nikishov spectrum [35], $\Phi\left(\kappa\right)$ is given by

$$\begin{aligned} \Phi(\kappa) = 0.18 & \left(\frac{\alpha_{th}^2 \chi_T}{\omega^2} \right) \frac{\left(\varepsilon \kappa^{-11}\right)^{-1/3}}{\pi} \left[1 + g\kappa^{\frac{2}{3}} \right] \\ & \times \left(\omega^2 \exp(-a\kappa^{\frac{4}{3}} - b\kappa^2) + d_r \exp(-c\kappa^{\frac{4}{3}} - d\kappa^2) - \omega(d_r + 1) \exp(-e\kappa^{\frac{4}{3}} - f\kappa^2) \right) \end{aligned} \tag{8}$$

where $a = 1.08 P_T^{-1} \eta_K^{4/3}$, $b = 1.692 P_T^{-1} \eta_K^2$, $c = 1.08 P_S^{-1} \eta_K^{4/3}$, $d = 1.692 P_S^{-1} \eta_K^2$, $e = 0.54 P_{TS}^{-1} \eta_K^{4/3}$, $f = 0.846 P_{TS}^{-1} \eta_K^2$ and $g = 2.35 \eta_K^{\frac{2}{3}}$. Here, η_K is Kolmogorov microscale length and given by $\eta_K = \left(\upsilon^3/\varepsilon\right)^{1/4}$ with υ referring to the kinematic viscosity. Furthermore, P_T is the Prandtl

number of temperature, P_S is the Prandtl number of salinity, P_{TS} is one half of the harmonic mean of P_T and P_S, and ω is the relative strength of temperature and salinity fluctuations. By replacing (8) inside (7) and expanding the zero-order Bessel function in terms of power series, we can express the wave structure function as

$$
\begin{aligned}
W(\rho,L) = {} & 1.44\pi k^2 L\alpha_{th}^2\chi_T\varepsilon^{(-1/3)}\int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(\rho\zeta)^{2n}}{(n!)^2\,2^{2n}}d\zeta\int_0^{\infty}\kappa^{2n-\frac{8}{3}}\exp\left(-a\kappa^{\frac{4}{3}}-b\kappa^2\right)d\kappa \\
& +1.44\pi k^2 L\left(\frac{\alpha_{th}^2\chi_T}{\omega^2}\right)d_r\varepsilon^{(-1/3)}\int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(\rho\zeta)^{2n}}{(n!)^2\,2^{2n}}d\zeta\int_0^{\infty}\kappa^{2n-\frac{8}{3}}\exp\left(-c\kappa^{\frac{4}{3}}-d\kappa^2\right)d\kappa \\
& -1.44\pi k^2 L\left(\frac{\alpha_{th}^2\chi_T}{\omega}\right)(d_r+1)\varepsilon^{(-1/3)}\int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(\rho\zeta)^{2n}}{(n!)^2\,2^{2n}}d\zeta\int_0^{\infty}\kappa^{2n-\frac{8}{3}}\exp(-e\kappa^{\frac{4}{3}}-f\kappa^2)d\kappa \\
& +1.44\pi k^2 L\alpha_{th}^2\chi_T\varepsilon^{(-1/3)}g\int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(\rho\zeta)^{2n}}{(n!)^2\,2^{2n}}d\zeta\int_0^{\infty}\kappa^{2n-2}\exp\left(-a\kappa^{\frac{4}{3}}-b\kappa^2\right)d\kappa \\
& +1.44\pi k^2 L\left(\frac{\alpha_{th}^2\chi_T}{\omega^2}\right)d_r\varepsilon^{(-1/3)}g\int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(\rho\zeta)^{2n}}{(n!)^2\,2^{2n}}d\zeta\int_0^{\infty}\kappa^{2n-2}\exp\left(-c\kappa^{\frac{4}{3}}-d\kappa^2\right)d\kappa \\
& -1.44\pi k^2 L\left(\frac{\alpha_{th}^2\chi_T}{\omega}\right)(d_r+1)\varepsilon^{(-1/3)}g\int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(\rho\zeta)^{2n}}{(n!)^2\,2^{2n}}d\zeta\int_0^{\infty}\kappa^{2n-2}\exp(-e\kappa^{\frac{4}{3}}-f\kappa^2)d\kappa
\end{aligned}
\tag{9}
$$

From (9), it can be observed that the first three integrals have similar forms. For the convenience of presentation, consider only the first integral. Using Eq. (4) of [36], Eq. (11.1) of [37], Eq. (9.2) of [37]), and Eq. (b) in [37, Ch. 9], we can define it in terms of the generalized hypergeometric function as

$$
\begin{aligned}
& \int_0^1\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(z\rho)^{2n}}{(n!)^2\,2^{2n}}\int_0^{\infty}\kappa^{2n-\frac{8}{3}}\exp\left(-a\kappa^{\frac{4}{3}}-b\kappa^2\right)d\kappa dz \\
& =\frac{1}{4}b^{\frac{5}{6}}\left\{2\Gamma\left(-\frac{5}{6}\right)\left[1-{}_2F_2\left(\frac{-5}{6},\frac{1}{2};1,\frac{3}{2},\frac{-\rho^2}{4b}\right)\right]+\frac{5a^3}{108b^2}\Gamma\left(\frac{-5}{6}\right)\left[1-{}_2F_2\left(\frac{7}{6},\frac{1}{2};1,\frac{3}{2},\frac{-\rho^2}{4b}\right)\right]\right\} \\
& -\frac{1}{4}ab^{\frac{1}{6}}\left\{2\Gamma\left(-\frac{1}{6}\right)\left[1-{}_2F_2\left(\frac{-1}{6},\frac{1}{2};1,\frac{3}{2},\frac{-\rho^2}{4R}\right)\right]+\frac{5a^3}{1296b^2}\Gamma\left(\frac{-1}{6}\right)\left[1-{}_2F_2\left(\frac{11}{6},\frac{1}{2};1,\frac{3}{2},\frac{-\rho^2}{4b}\right)\right]\right\} \\
& +\frac{1}{8}a^2b^{\frac{-1}{2}}\left\{2\Gamma\left(\frac{1}{2}\right)\left[1-{}_2F_2\left(\frac{1}{2},\frac{1}{2};1,\frac{3}{2},\frac{-\rho^2}{4b}\right)\right]-\frac{a^3}{40b^2}\Gamma\left(\frac{1}{2}\right)\left[1-{}_2F_2\left(\frac{5}{2},\frac{1}{2};1,\frac{3}{2},\frac{-\rho^2}{4b}\right)\right]\right\}
\end{aligned}
\tag{10}
$$

where ${}_pF_q\left(a_1,\cdots\right.$ $\cdots$ is the generalized hypergeometric function, with p and q being positive integers and $\Gamma(\bullet$ is Gamma function. Noting $\mathrm{Re}\left(-\rho^2/4b\right)\gg$ and based on

the asymptotic behavior of hypergeometric function, i.e., Eq. (8) of [38], we can approximate (10) as

$$\int_0^1 \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(z\rho)^{2n}}{(n!)^2 2^{2n}} \int_0^{\infty} \kappa^{2n-\frac{8}{3}} \exp\left(-a\kappa^{\frac{4}{3}} - b\kappa^2\right) d\kappa dz \approx -\frac{1}{2} b^{\frac{5}{6}} \Gamma\left(\frac{-5}{6}\right) \frac{\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{4}{3}\right)}{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{11}{6}\right)\Gamma\left(\frac{7}{3}\right)} \left(\frac{\rho^2}{4b}\right)^{\frac{5}{6}}$$

$$= 0.4194\rho^{\frac{5}{3}} \tag{11}$$

Similarly, it can be shown that the second and third integrals yield $0.4194\rho^{\frac{5}{3}}$.

Now, we consider the last three integrals which have also identical forms. For the convenience of presentation, consider only the fourth integral. Using Eq. (5) of [36], this can be expressed as

$$\int_0^1 \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(z\rho)^{2n}}{(n!)^2 2^{2n}} \int_0^{\infty} \kappa^{2n-2} \exp\left(-a\kappa^{\frac{4}{3}} - b\kappa^2\right) d\kappa dz \tag{12}$$

$$= \frac{1}{2} b^{\frac{1}{2}} \left\{ \Gamma\left(-\frac{1}{2}\right)\left[1 - {}_2F_2\left(\frac{-1}{2}, \frac{1}{2}; 1, \frac{3}{2}, \frac{-\rho^2}{4b}\right)\right] + \frac{a^3}{24b^2}\Gamma\left(\frac{-1}{2}\right)\left[1 - {}_2F_2\left(\frac{3}{2}, \frac{1}{2}; 1, \frac{3}{2}, \frac{-\rho^2}{4b}\right)\right] \right\}$$

$$- \frac{1}{2} a b^{-\frac{1}{6}} \left\{ \Gamma\left(\frac{1}{6}\right)\left[1 - {}_2F_2\left(\frac{1}{6}, \frac{1}{2}; 1, \frac{3}{2}, \frac{-\rho^2}{4b}\right)\right] - \frac{7a^3}{864b^2}\Gamma\left(\frac{1}{6}\right)\left[1 - {}_2F_2\left(\frac{13}{6}, \frac{1}{2}; 1, \frac{3}{2}, \frac{-\rho^2}{4b}\right)\right] \right\}$$

$$+ \frac{1}{4} a^2 b^{\frac{-5}{6}} \left\{ \Gamma\left(\frac{5}{6}\right)\left[1 - {}_2F_2\left(\frac{5}{6}, \frac{1}{2}; 1, \frac{3}{2}, \frac{-\rho^2}{4b}\right)\right] - \frac{11a^3}{432b^2}\Gamma\left(\frac{5}{6}\right)\left[1 - {}_2F_2\left(\frac{17}{6}, \frac{1}{2}; 1, \frac{3}{2}, \frac{-\rho^2}{4b}\right)\right] \right\}$$

Noting $\mathrm{Re}\left(-\rho^2/4b\right) \gg$ and using the asymptotic behavior of hypergeometric function i.e., Eq. (8) of [38], we have

$$\int_0^1 \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(z\rho)^{2n}}{(n!)^2 2^{2n}} \int_0^{\infty} \kappa^{2n-2} \exp\left(-a\kappa^{\frac{4}{3}} - b\kappa^2\right) d\kappa dz \approx -\frac{1}{2} b^{\frac{1}{2}} \frac{\Gamma\left(-\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2}\right)} \left(\frac{\rho^2}{4b}\right)^{\frac{1}{2}} \tag{13}$$

$$= 0.5\rho$$

Replacing $0.4194\rho^{5/3}$ as the solution of first three integrals and 0.5ρ as the solution of last three integrals, we obtain the final form of wave structure function as

$$W(\rho, L) = 1.44\pi k^2 L \left(\frac{\alpha_{th}^2 \chi_T}{\omega^2}\right) \varepsilon^{-\frac{1}{3}} \left(1.175\eta_K^{2/3}\rho + 0.419\rho^{\frac{5}{3}}\right)\left(\omega^2 + d_r - \omega\left(d_r + 1\right)\right) \tag{14}$$

This can be now replaced in (6) to calculate the average power transfer over the underwater quantum link which is required for the calculation of QBER bound in (4).

As a benchmark, we further consider a QKD system operating in non-turbulent conditions. The exact QBER of such a QKD system is given by [31]

$$\mathrm{QBER}_{non} = \frac{2n_N}{n_S \mu_0 l + 4n_N} \tag{15}$$

where μ_0 is the largest eigenvalue of the singular value decomposition of vacuum-propagation Green's function given in [39].

As a sanity check, we consider two special cases. First, we assume large values of extinction coefficient ς where turbidity effects are more pronounced. For sufficiently large ς values, (5) can be simplified as $l \approx 0$ and consequently we have $\exp(-\eta n_S l) \cong 1$. Furthermore, we assume $\mu \cong \mu_0$ which can be justified for sufficiently short distances where the effect of turbulence is negligible. Replacing these within the derived upper bound on QBER, we obtain

$$\mathrm{QBER} \cong \frac{2n_N}{\mu n_S l + 4n_N} \tag{16}$$

which coincides with (15) for the non-turbulent case. This result shows that the effect of turbulence is negligible when turbidity is dominant. As a second case, we assume $\mu \cong \mu_0 = 1$ which can be justified for short distances in the presence of very weak turbulence. Replacing it within (4), we again revert to the non-turbulence case. In other words, when the transmitted photons experience weak turbulence at short distances, the influence of path loss is dominant as expected.

III.b. SKR Analysis

SKR is defined as the difference between the amount of information shared by Alice and Bob and the amount of residual information that Eve might have [30]. For BB84 protocol, the quantum channel can be modeled as a binary symmetric channel (BSC) with crossover probability of QBER . The minimum amount of information that should be sent from Alice to Bob in order to correct his key string can be described by the entropy function $h(\mathrm{QBER}) = -\mathrm{QBER}\log_2(\mathrm{QBER}) - (1-\mathrm{QBER})\log_2(1-\mathrm{QBER})$ [40]. The amount of

disclosed information to Eve in this process can be then expressed as $1-h(\mathrm{QBER})$ [40]. Therefore, SKR for BB84 protocol can be written as [40]

$$R=1-(1+f)h(\mathrm{QBER}) \tag{17}$$

where f is the reconciliation efficiency [40] and its value depends on the employed error correction code.

In our work, we consider low density parity check (LDPC) codes optimized for BSCs [40]. The corresponding reconciliation efficiency is given by [41]

$$f=\frac{1-R_c}{h(\mathrm{QBER}_{th})} \tag{18}$$

where R_c is the code rate and QBER_{th} is a threshold value preset in LDPC code design [42], i.e., this corresponds to the maximum value of QBER that can be corrected as the code length tends to infinity. The code rates and threshold QBER values for optimized LDPC codes can be found in Table 1 of [40].

Replacing (18) in (17) and using the upper bound on QBER in (4), a lower bound on SKR is obtained as

$$R\geq 1-\left(1+\frac{1-R_c}{h(\mathrm{QBER}_{th})}\right)h\left(\frac{n_N\left(1-\mu+\mu e^{-\eta n_S l}\right)}{\frac{n_S l}{2}\mu e^{-\eta n_S l}+2n_N\left(1-\mu+\mu e^{-\eta n_S l}\right)}\right)$$

IV. Numerical Results

In this section, we demonstrate the performance of underwater QKD scheme under consideration. We assume transmitter beam divergence angle of $\theta=6^{\circ}$, dark current count rate of $I_{dc}=60$ Hz, filter spectral width of $\Delta\lambda=0.12\times10^{-9}$ nm, bit period of $\Delta t=35$ ns, receiver gate time of $\Delta t'=200$ ps, and Geiger-mode APD quantum efficiency of $\eta=0.5$. Unless otherwise stated, we assume an average photon number of $n_S=1$, transmitter and receiver aperture diameters of $d_1=d_2=10$ cm, FOV of $\Omega=180^{\circ}$ and clear atmospheric conditions at night with a full moon. We consider clear ocean, coastal water, and harbor water as water types. As for channel parameters, we assume $\alpha_{th}=2.56\times10^{-4}$ 1/deg, $P_T=7$, $P_S=6.86\times10^{2}$, $P_{TS}=13.85$ and $\upsilon=1.0576\times10^{-6}$ $\mathrm{m^2s^{-1}}$ [35]. We consider three representative cases for

turbulence strength. Specifically, we assume $\omega = -2.2$, $\chi_T = 2\times10^{-7}$ K^2s^{-3} and $\varepsilon = 2\times10^{-5}$ m^2s^{-3} for weak turbulence, $\omega = -2.2$, $\chi_T = 1\times10^{-6}$ K^2s^{-3} and $\varepsilon = 5\times10^{-7}$ m^2s^{-3} for moderate turbulence and $\omega = -2.2$, $\chi_T = 10^{-5}$ K^2s^{-3} and $\varepsilon = 10^{-5}$ m^2s^{-3} for strong oceanic turbulence [43]. For the convenience of the reader, the channel and system parameters are summarized in Table 1.

Effect of water type: Fig. 2 illustrates the upper bound on QBER and the lower bound on SKR with respect to link distance for clear ocean, coastal water and turbid water. For each water type, we assume weak, moderate and strong turbulence. It can be observed from Fig. 2.a. that the turbulence effect in turbid water is negligible and the path loss is the dominant factor which verifies our discussion in Section III. For example, if $\text{QBER} \leq 0.11$ is targeted[1], we have the same achievable distance of 6 m regardless of the level of turbulence. As turbidity decreases, the achievable distance increases and the effect of turbulence is more pronounced. The QBER performance for non-turbulent case in (15) is also included as a benchmark. In non-turbulent coastal water, the achievable distance to maintain $\text{QBER} \leq 0.11$ is around 60 m and reduces to 54 m for strong turbulence. For clear ocean, the achievable distance for weak turbulence and non-turbulent conditions is the same and around 155 m confirming our earlier discussion in Section III. The achievable distance reduces to 128 m and 107 m for moderate and strong turbulence, respectively.

The aforementioned achievable distances are possible under the assumption of perfect error correction. In an effort to have an insight into what transmission distances can be obtained with practical coding schemes, Fig. 2.b depicts the SKR performance against the link length. We employ an LDPC code[2] with a rate of $R_c = 0.5$ optimized for a BSC channel with crossover probability of $\text{QBER}_{th} = 0.1071 \approx 0.11$ [40]. It can be observed that the maximum distance to support a non-zero SKR value for turbid water (regardless of turbulence level) is 5 m. This is obviously less than the achievable distance of 6 m obtained through QBER analysis. Similarly,

[1] It is generally accepted that for BB84 protocol is secure against a sophisticated quantum attack if QBER is less than 0.11 [44].

[2] In our numerical results, we keep the code rate fixed and employ the LDPC code optimized for QBER threshold value of 0.11. It is also possible to use other LDPC codes in [40] optimized for lower QBER values. This will improve SKR, however, the maximum transmission distance will still remain the same because the highest QBER that can be tolerated to obtain non-zero SKR should be less than 0.11.

it can be readily checked that the maximum distances to support a non-zero SKR value for other combinations of water type and turbulence level are slightly smaller than achievable distances earlier obtained. For example, the maximum transmission distances for coastal water and clear water in weak turbulence conditions are 59 m and 153 m while corresponding QBER analysis yields 60 m and 155 m.

Effect of atmospheric condition: In Fig. 3, we investigate the effect of different atmospheric conditions on the performance of the QKD system. We consider clear ocean with strong turbulence and assume clear, hazy and overcast atmosphere with relative locations of sun and earth at day time. As a benchmark, clear atmospheric conditions at night with a full moon (assumed in Fig. 2) is also included. It can be observed from Fig. 3 that the achievable distance for underwater QKD system at day time drastically reduces in comparison to night time conditions due to an increase in the received background noise. For example, when the sun is near horizon, the maximum transmission distance (obtained through SKR analysis) for the heavy overcast atmosphere is 49 m while it reduces to 21 m and 6 m respectively for heavy overcast atmosphere and for clear atmosphere with the sun at zenith location. These are much lower than 106 m achievable under the same system assumptions at night with a full moon.

Effect of FOV: In Fig. 4, we investigate the effect of FOV on the performance of the QKD system. We assume clear ocean with strong turbulence and consider two atmospheric cases. These are clear weather night with a full moon and heavy overcast when sun is near the horizon. We assume $\Omega = 10^{\circ}$, 60° and 180°. It is observed that at night time, the effect of FOV is practically negligible and the QBER remains the same for all FOV values under consideration. Benefit of choosing a proper value of FOV becomes clear as the environment irradiance increases. In daylight, we observe that the achievable distance significantly improves as the FOV decreases. This improvement is due to the decrease in background noise as the FOV decreases. Mathematically speaking, the maximum transmission distance (obtained through SKR analysis) for $\Omega = 180^{\circ}$ is around 49 m, while it increases to 62 m and 93 m for $\Omega = 60^{\circ}$ and 10°, respectively.

Effect of aperture size: In Fig. 5, we study the effect of aperture size on the performance of underwater QKD system. Similar to Fig. 4, we assume clear ocean with strong turbulence

and consider two distinct atmospheric conditions. We assume the receiver aperture size varies as $d_2 =$ 10, 20 and 30 cm and the transmitter pupil has the same diameter as the receiver. It is observed that at night time with a full moon, the achievable distance increases as the diameter size increases. For example, the maximum transmission distance (obtained through SKR analysis) for $d_2 =$ 10 cm is around 106 m, while it climbs up to 128 m and 151 m for $d_2 =$20 cm and 30 cm, respectively. It should be emphasized that the increase in background noise as a result of increasing the diameter size is negligible at night. On the other hand, at daylight, increasing the diameter size has a negative effect on the performance. It is observed that the maximum transmission distance for $d_2 =$10 cm is 49 m, whereas it decreases to 38 m and 27 m for diameter size of 20 and 30 cm, respectively. These observations indicate the necessity of using adaptive selection of aperture size in practical implementations.

V. Conclusions

In this paper, we have investigated the performance of the BB84 protocol over turbulent underwater channels. Our results have demonstrated that the turbulence effect in turbid water is negligible and the path loss is the dominant factor. As turbidity decreases, the achievable distance increases and the effect of turbulence is more pronounced. Our results have further shown that achievable distance for underwater QKD system at day time drastically reduces in comparison to night time due to an increase in the received background noise. We have also investigated the effect of system parameters such as aperture size and FOV on QBER and SKR performance. At night time, the effect of FOV has been found to be practically negligible and the performance remains the same for all FOV values under consideration. In daylight, the achievable distance significantly improves as the FOV, and therefore background noise, decreases. It has been also observed that when the aperture size increases the achievable distance increases at night time while it decreases at daylight. Such observations indicate the necessity of using adaptive selection of aperture size in practical implementations.

References

[1] M. Erol-Kantarci, H.T. Mouftah, and S. Oktug, "A survey of architectures and localization techniques for underwater acoustic sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp.487-502, 2011.

[2] https://www.l3oceania.com, "AUSSNe," 2012. [Online]. Available: https://www.l3oceania.com/mission-systems/maritime-domain-awareness/aussnet.aspx.

[3] https://www.nec.com, "Harbor Monitoring Network System," 2015. [Online]. Available: https://www.nec.com/en/global/solutions/safety/critical_infra/harbormonitoring.html. [Accessed: 16-August- 2019] check again

[4] A. Caiti, V. Calabrò, A. Munafò, G. Dini, and A. Lo Duca, "Mobile Underwater Sensor Networks for Protection and Security: Field Experience at the UAN11 Experiment", *Wiley Journal of Field Robotics*, vol. 30, no. 2, pp. 237–253, 2013.

[5] M. Ibragimov, J.H. Lee, M. Kalyani, J.I. Namgung, S.H. Park, O. Yi, C.H. Kim, and Y.K. Lim, "CCM-UW security modes for low-band underwateracoustic sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 479–499, Jul. 2016

[6] G. Han, J. Jiang, N. Sun and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54-60, 2015.

[7] M.A. Nielsen, and I. Chuang, *Quantum computation and quantum information*, Cambridge: Cambridge Univ. Press, 2002.

[8] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process*, Bengaluru, India, Dec. 1984, pp. 175–179.

[9] A.K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.

[10] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons" *Phys. Rev. Lett.*, vol. 84, no. 20, p. 4729, 2000.

[11] J. Yin, Y. Cao, Y.H. Li, S.K. Liao, L. Zhang, J.G. Ren, W.Q. Cai, W.Y. Liu, B. Li, H. Dai, and G.B. Li, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140-1144, 2017.

[12] E.Y. Zhu, C, Corbari, A. Gladyshev, P.G. Kazansky, H.K. Lo, and L. Qian, "Toward a reconfigurable quantum network enabled by a broadband entangled source," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B1-B6, 2019.

[13] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," *New J. Phys.*, vol. 8, no. 5, p. 75, 2006.

[14] M. Mirhosseini, O.S. Magaña-Loaiza, M.N. O'Sullivan, B. Rodenburg, M. Malik, M.P. Lavery, M.J. Padgett, D.J. Gauthier, and R.W. Boyd, "High-dimensional quantum cryptography with twisted light," *New J. Phys.*, vol. 17, no. 3, p. 033033, 2015.

[15] E. Diamanti, H.K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Inf.*, vol. 2, pp. 16025, 2016.

[16] S.C. Zhao, X.H. Han, Y. Xiao, Y. Shen, Y.J. Gu, and W.D. Li, "Performance of underwater quantum key distribution with polarization encoding," *J. Opt. Soc. Am. A*, vol. 36, no. 5, pp. 883-892, 2019.

[17] M. Lanzagorta, and J. Uhlmann, "Assessing Feasibility of Secure Quantum Communications Involving Underwater Assets," *IEEE J. Ocean. Eng.*, 2019.

[18] P. Shi, S. C. Zhao, Y. J. Gu, and W. D. Li, "Channel analysis for single photon underwater free space quantum key distribution," *J. Opt. Soc. Am. A*, vol. 32, no. 3, pp. 349-356, 2015.

[19] M. Lopes, and N. Sarwade, "Optimized decoy state QKD for underwater free space communication," *International Journal of Quantum Information*, vol. 16, no. 02, p. 1850019, 2018.

[20] F. Bouchard, K. Heshami, D. England, R. Fickler, R.W. Boyd, B.G. Englert, L.L. Sánchez-Soto, and E. Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," *Quantum*, vol. 2, p. 111, 2018.

[21] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over a water channel," *Appl. Opt.,* vol. 58, no. 14, pp. 3902-3907, 2019.

[22] C.Q. Hu, Z.Q. Yan, J. Gao, Z.Q. Jiao, Z.M. Li, W.G. Shen, Y. Chen, R.J. Ren, L.F. Qiao, A.L. Yang, and H. Tang, "Transmission of photonic polarization states through 55-m water: towards air-to-sea quantum communication," *Photonics Research*, vol. 7, no. 8, pp. A40-A44, 2019.

[23] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Opt. Exp.*, vol. 26, no. 17, pp. 22563-22573, 2018.

[24] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B.J. Sussman, R.W. Boyd, et al., "Characterization of an underwater channel for quantum communications in the Ottawa River," *Opt. Express,* vol. 27, pp. 26346-26354, 2019.

[25] J. Gariano, and I.B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Opt. Exp.*, vol. 27, no. 3, pp. 3055-3064, 2019.

[26] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.,* vol. 74, no. 1, pp. 145–195, 2002.

[27] M. Lanzagorta, *Underwater communications,* San Rafael, CA, USA: Morgan & Claypool, 2013.

[28] C. Mobley, *Light and Water: Radiative Transfer in Natural Waters*, Academic Press, 1994.

[29] C. Mobley, E. Boss, and C. Roesler, "Ocean Optics Web Book," 2010. [Online]. Available: http://www.oceanopticsbook.info

[30] C. Kollmitzer, and M. Pivk, *Applied quantum cryptography*, vol. 797. Berlin, Germany: Springer, 2010.

[31] J.H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Phys. Rev. A*, vol. 67, no. 2, pp. 022309, 2003.

[32] F. Hanson, and S. Radic, "High bandwidth underwater optical communication," *Appl. Opt.*, vol. 47, no. 2, pp. 277-283, 2008.

[33] M. Elamassie, F. Miramirkhani, and M. Uysal, "Performance characterization of underwater visible light communication," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 543-552, 2019.

[34] L. C. Andrews, and R. L. Phillips, *Laser Beam Propagation through Random Media*, Bellingham, WA, USA: SPIE, 2005.

[35] M. Elamassie, M. Uysal, Y. Baykal, M. Abdallah, and K. Qaraqe, "Effect of eddy diffusivity ratio on underwater optical scintillation index," *J. Opt. Soc. Am. A*, vol. 34, no. 11, pp. 1969–1973, 2017.

[36] L. Lu, X. Ji, and Y. Baykal, "Wave structure function and spatial coherence radius of plane and spherical waves propagating through oceanic turbulence," *Opt. Exp.*, vol. 22, no. 22, pp. 27112-27122, 2014.

[37] L.C. Andrews, *Special functions of mathematics for engineers*, New York, NY, USA: McGraw-Hill, 1992.

[38] L.C. Andrews, S. Vester, and C.E. Richardson, "Analytic expressions for the wave structure function based on a bump spectral model for refractive index fluctuations," *J. Mod. Opt.*, vol. 40, no. 5, pp. 931–938, 1993.

[39] D. Slepian, "Analytic solution of two apodization problems," *J. Opt. Soc. Am.*, vol. 55, no. 9, pp. 1110–1115, 1965.

[40] D. Elkouss, A. Leverrier, R. Alleaume, and J.J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2009, pp. 1879–1883.

[41] J. Martinez-mateo, D. Elkouss, and V. Martin, "Blind Reconciliation," *Quantum Inf. Comput.*, vol. 12, no. 9, pp.0791-0812, 2012.

[42] T.J. Richardson, and R.L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599-618, 2001.

[43] T. Wu, X. Ji, H. Zhang, X. Li, L. Wang, and X. Fan, "Rytov variance of spherical wave and performance indicators of laser radar systems in oceanic turbulence," *Opt. Commun.*, vol. 434, pp. 36-43, 2019.

[44] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.

Table 1 System and channel parameters

Parameter	**Definition**		**Numerical Value**
Ω	Field of view		180° [33]
$\Delta\lambda$	Filter spectral width		0.12×10^{-9} nm [27]
λ	Wavelength		530 nm [33]
Δt	Bit period		35 ns [27]
$\Delta t'$	Receiver gate time		200 ps [27]
d_1	Transmitter aperture diameter		10 cm [31]
d_2	Receiver aperture diameter		10 cm [31]
η	Quantum efficiency		0.5 [31]
I_{dc}	Dark current count rate		60 hz [27]
K_{∞}	Asymptotic diffuse attenuation coefficient		0.08 m^{-1} [29]
z_d	Depth		100 m [27]
θ	Transmitter beam divergence angle		6° [33]
ς	Extinction coefficient	Clear water	0.151 m^{-1} [32]
		Coastal water	0.339 m^{-1} [32]
		Turbid harbor	2.195 m^{-1} [32]
T	Correction coefficient	$\theta=6^{\circ}$, $d_1=10\,\mathrm{cm}$	0.16 [33]
		$\theta=6^{\circ}$, $d_1=20\,\mathrm{cm}$	0.21 [33]
		$\theta=6^{\circ}$, $d_1=30\,\mathrm{cm}$	0.26 [33]

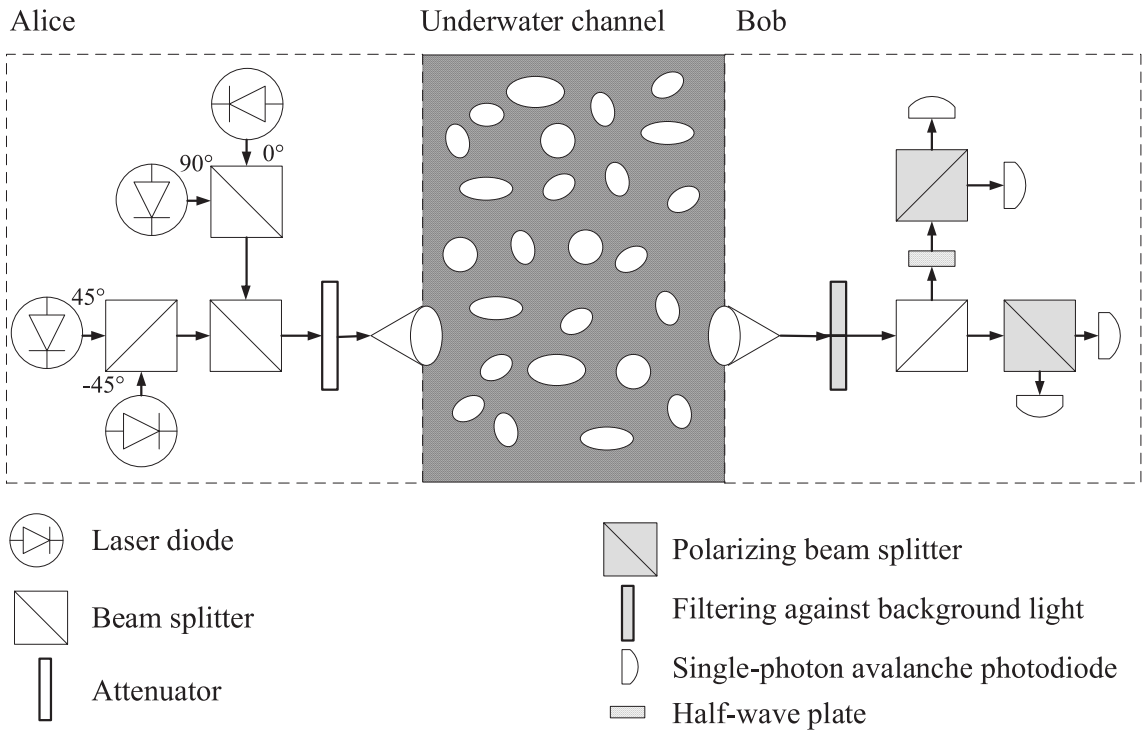
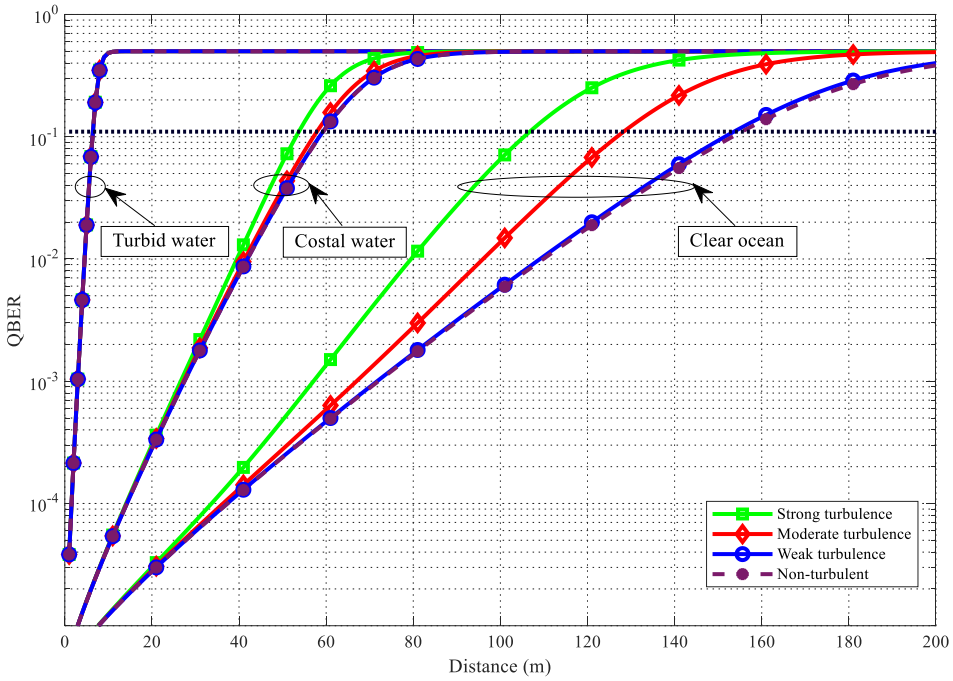
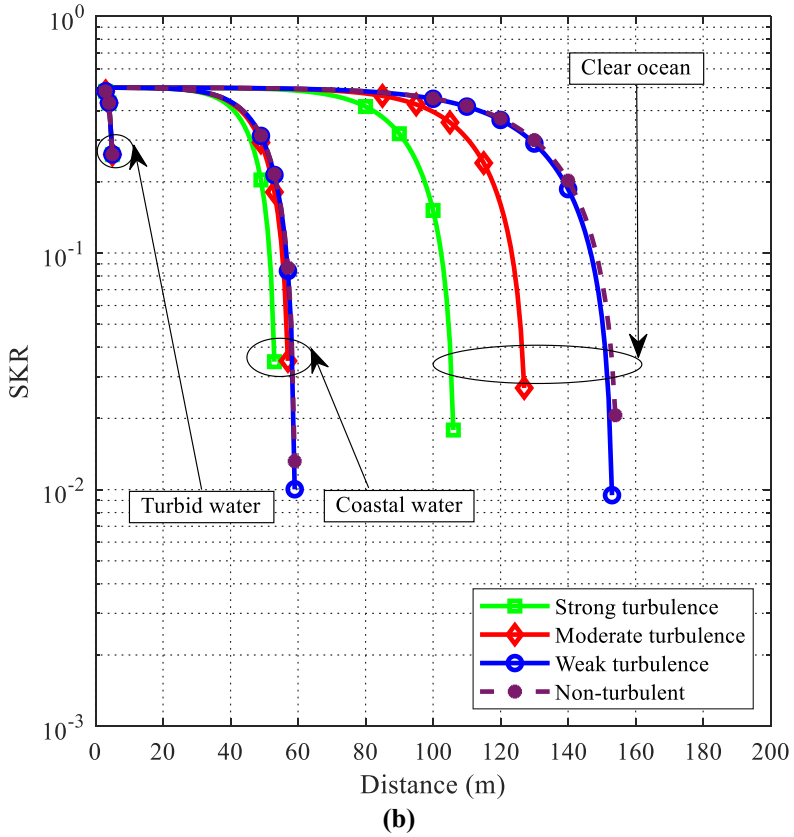


Fig. 1 Underwater BB84 QKD system under consideration

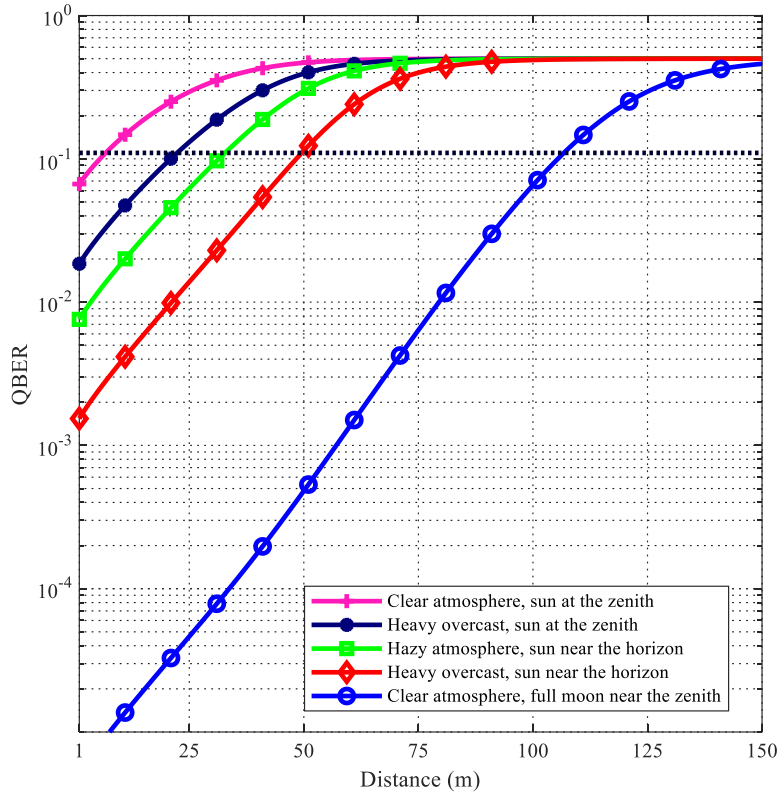


(a)

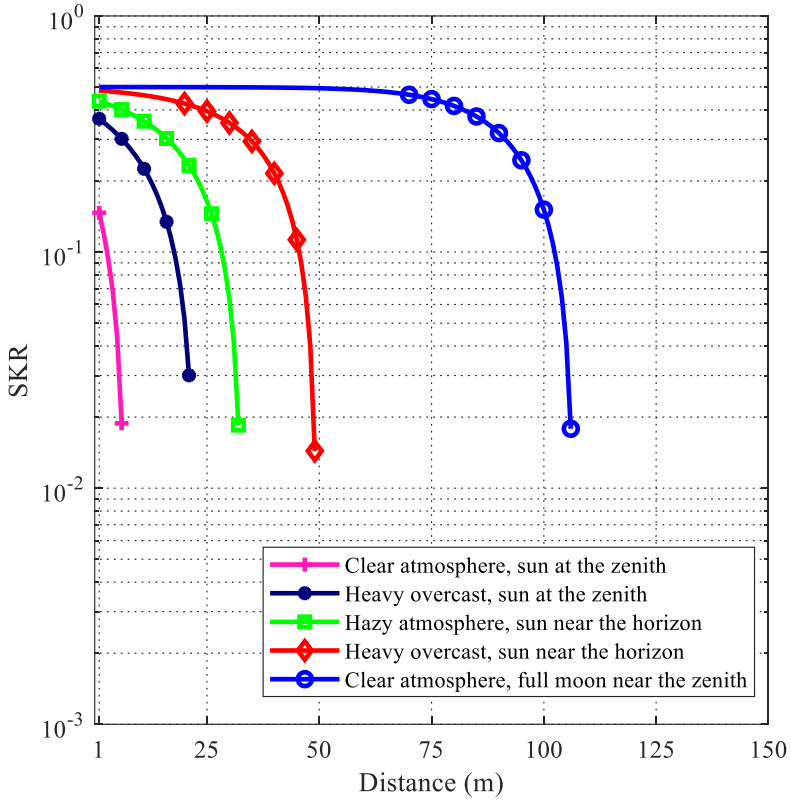


(b)

Fig. 2 Effect of turbulence strength for different water types at night time with a full moon on (a) QBER (b) SKR

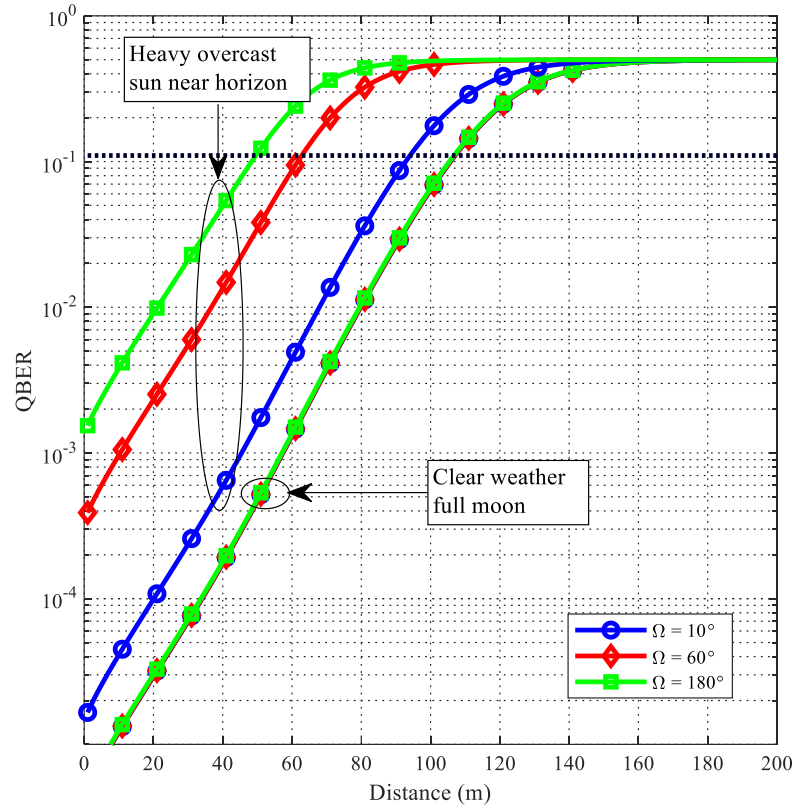


(a)

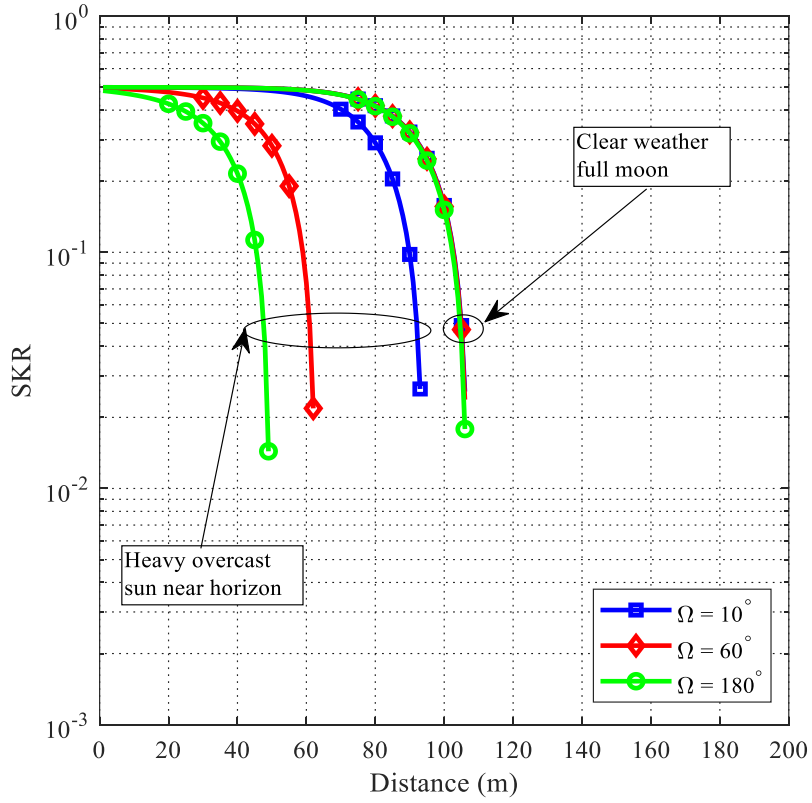


(b)

Fig. 3 Effect of atmospheric condition in clear ocean with strong turbulence on (a) QBER (b) SKR

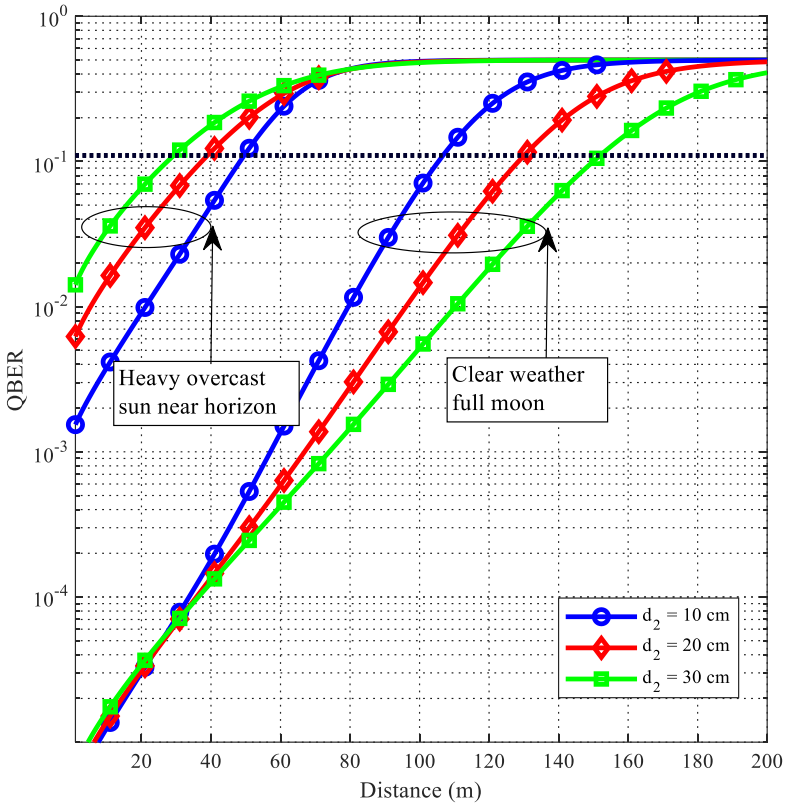


(a)

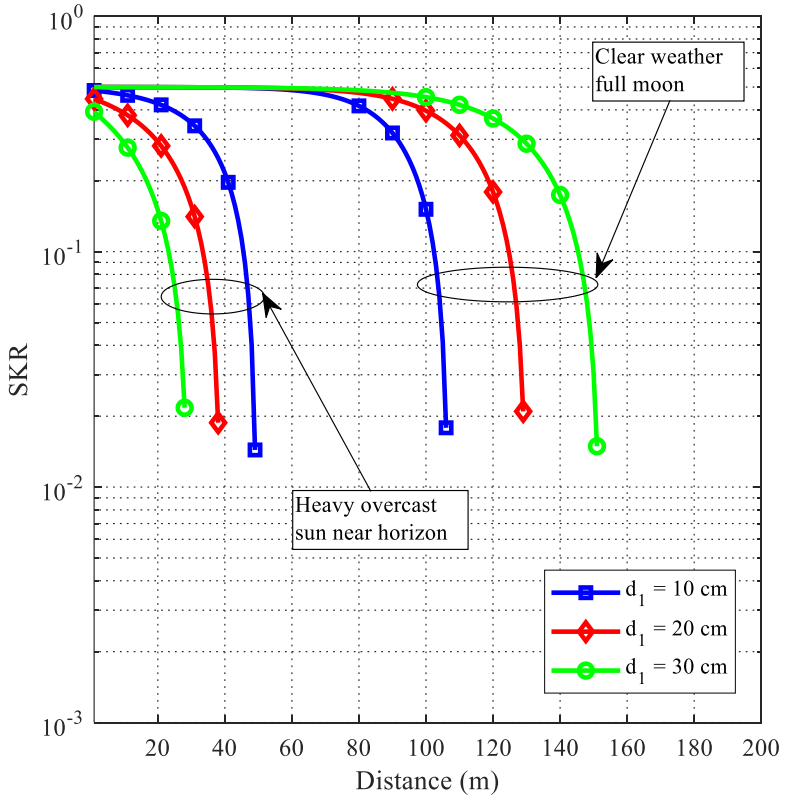


(b)

Fig. 4 Effect of field of view in clear ocean with strong turbulence under different atmospheric conditions on (a) QBER (b) SKR



(a)



(b)

Fig. 5 Effect of aperture size in clear ocean with strong turbulence under different atmopsheric conditions on (a) QBER (b) SKR